WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Wednesday, April 27, 2005

Hide?	Set Name	Query	Hit Count
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
☐	L28	L7 and "zero knowlege protocol"	0
☐	L27	L7 and "zero-knowlege-protocol"	0
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
☐	L26	L7 and zero$	51
☐	L25	L24 and l21	9
☐	L24	L19 and zero$	20
☐	L23	L19 and "zero knowlege protocol"	0
☐	L22	L19 and "zero-knowlege-protocol"	0
☐	L21	L19 and (authentic$ with (encrypt$ or crypto$ or decrypt$))	16
☐	L20	L19 and (encrypt$ or crypto$ or decrypt$)	25
☐	L19	L18 and l7	45
☐	L18	l17 or l16 or l15 or l14 or l13 or l10 or l9 or l8	19765
☐	L17	235/492,380,375,385.ccls.	6543
☐	L16	713/169,173,176,180,178.ccls.	1873
☐	L15	380/30,46,200,202,54.ccls.	2046
☐	L14	283/901.ccls.	447
☐	L13	235/375,385,380.ccls.	5045
☐	L12	235/375,385,380.ccls.L11	8847
☐	L11	283/901.ccls.L10	3812
☐	L10	382/232,260,270,284.ccls.	3366
☐	L9	340/5.8,5.86.ccls.	588
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
☐	L8	705/67,26-27,51,57.ccls.	6004
☐	L7	=19980414	197
☐	L6	(authentic$ with (product or article or item or goods)) and ((fake$ or counterfeit$ or "anti-conterfeit") same (authentic$ with (product or article or item or goods)))	717
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
☐	L5	L3 not l4	1

☐	L4	L3 and (zero$)	9
☐	L3	L2 and (authentic$ with (product or article or item or goods)) and l1	10
☐	L2	(electronic$ or smart$) adj2 tag	809
☐	L1	=19980414	1211487

END OF SEARCH HISTORY

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 10 of 16 returned.

☐ 1. Document ID: US 6600823 B1

Using default format because multiple data bases are involved.

L21: Entry 1 of 16 File: USPT Jul 29, 2003

US-PAT-NO: 6600823
DOCUMENT-IDENTIFIER: US 6600823 B1

TITLE: Apparatus and method for enhancing check security

DATE-ISSUED: July 29, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hayosh; Thomas D.	Bloomfield Hills	MI		

US-CL-CURRENT: 380/51; 380/55, 713/170, 713/176, 713/179

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 2. Document ID: US 6363483 B1

L21: Entry 2 of 16 File: USPT Mar 26, 2002

US-PAT-NO: 6363483
DOCUMENT-IDENTIFIER: US 6363483 B1

TITLE: Methods and systems for performing article authentication

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 3. Document ID: US 6069955 A

L21: Entry 3 of 16 File: USPT May 30, 2000

US-PAT-NO: 6069955
DOCUMENT-IDENTIFIER: US 6069955 A

TITLE: System for protection of goods against counterfeiting

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 4. Document ID: US 5878142 A

L21: Entry 4 of 16 File: USPT Mar 2, 1999

US-PAT-NO: 5878142
DOCUMENT-IDENTIFIER: US 5878142 A

TITLE: Pocket encrypting and authenticating communications device

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 5. Document ID: US 5666417 A

L21. Entry 5 of 16 File: USPT Sep 9, 1997

US-PAT-NO: 5666417
DOCUMENT-IDENTIFIER: US 5666417 A

TITLE: Fluorescence authentication reader with coaxial optics

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 6. Document ID: US 5640002 A

L21: Entry 6 of 16 File: USPT Jun 17, 1997

US-PAT-NO: 5640002
DOCUMENT-IDENTIFIER: US 5640002 A

TITLE: Portable RF ID tag and barcode reader

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 7. Document ID: US 5574790 A

L21: Entry 7 of 16 File: USPT Nov 12, 1996

US-PAT-NO: 5574790
DOCUMENT-IDENTIFIER: US 5574790 A

TITLE: Fluorescence authentication reader with coaxial optics

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 8. Document ID: US 5546463 A

L21: Entry 8 of 16 File: USPT Aug 13, 1996

US-PAT-NO: 5546463
DOCUMENT-IDENTIFIER: US 5546463 A

TITLE: Pocket encrypting and authenticating communications device

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

☐ 9. Document ID: US 5418855 A

L21: Entry 9 of 16 File: USPT May 23, 1995

US-PAT-NO: 5418855
DOCUMENT-IDENTIFIER: US 5418855 A

TITLE: Authentication system and method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

☐ 10. Document ID: US 5303370 A

L21: Entry 10 of 16 File: USPT Apr 12, 1994

US-PAT-NO: 5303370
DOCUMENT-IDENTIFIER: US 5303370 A

TITLE: Anti-counterfeiting process using lenticular optics and color masking

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L19 and (authentic$ with (encrypt$ or crypto$ or decrypt$))	16

Display Format: - Change Format

Previous Page Next Page Go to Doc#

L21: Entry 11 of 16 File: USPT Feb 21, 1989

DOCUMENT-IDENTIFIER: US 4807287 A
TITLE: Document authentication method

Abstract Text (1):
A system for authenticating a document includes a uniqueness characteristic reader to generate a first identifier for the document. The identifier is then encrypted and optionally encoded to define an error correction code. The encrypted identifier and the optional error correction code are combined in accordance with a predefined format to define a code which is stored on the document itself (such as on a magnetic stripe). Authentication of the document is accomplished by reading the code on the item. The code is then processed to identify the location and quantity of any erroneous data. The identified location and quantity information for erroneous data, in conjunction with the optional error correction code, is then utilized to correct all errors in at least the encrypted identifier portion of the code read from the storage medium. The resultant encrypted identifier is therefore retrieved from the storage medium on the item without error. The retrieved encrypted identifier is then decrypted to retrieve the first identifier. A second item identifier is generated by reading the uniqueness characteristic from the document in the same manner that the first item identifier was generated. The second item identifier is then compared with the retrieved identifier from the document with the document being authenticated when the retrieved identifer compares with the second item identifier according to a predefined compare criteria.

Application Filing Date (1):
19870406

Brief Summary Text (2):
The present invention relates to a system for self authenticating an item of value, and in particular, to a system for authenticating items by retrieving authenticating data from a storage medium such as a magnetic stripe disposed on the item of value, even if the storage medium has been physically damaged.

Brief Summary Text (3):
Numerous systems have been devised for authenticating articles, particularly those vulnerable to being counterfeited. Examples include imprinting an object with a difficult to copy pattern, application of holographic tape and marking the item with secret identification indicia.

Brief Summary Text (4):
One particularly effective method and apparatus for authenticating articles is described in U.S. Pat. No. 4,423,415, issued Dec. 27, 1983, to Goldman and entitled "Non-Counterfeitable Document System." Although, the Goldman system is effective, additional security may be desired if the item to be authenticated is a high value document such as a stock certificate or bond. One means of increasing security is to encrypt the identifier in a manner such as described in U.S. Pat. No. 4,405,829 entitled "Cryptographic Communications System and Method" issued Sept. 20, 1983, to Rivest et al.

Brief Summary Text (7):

One means of storing very large quantities of information in a small space is to place a machine readable magnetic stripe on the item itself. However, practical use of a magnetic stripe to store data on a document presently requires that the stripe be printed directly onto the document. Because documents are generally made out of paper and paper has a highly irregular surface contour, a printed magnetic stripe will exhibit a highly irregular geometry which cause wide variations in the magnetic flux characteristic along the length of the stripe. Heretofore, such wide variations in magnetic flux characteristics have resulted in the inability to retrieve data accurately or reliably - an essential requirement when encrypted data is stored to verify authenticity.

Brief Summary Text (11):
Therefore, there is a need for an authentication system which includes a document with a storage medium such as a magnetic stripe printed directly on its surface and capable of storing large quantities of data, at least a portion of which data is preferably encrypted, and from which the stored data can be retrieved without errors, even in the presence of physical damage such as tears, folds or scratches, thereby enabling decryption and authenticity verification. The storage medium (stripe) is preferably of the type that is applied by offset printing so as to be highly compatible with the printing of the remaining information on the document of value.

Brief Summary Text (13):
In accordance with the present invention, a document, such as a stock certificate or bond having a significant value, may be authenticated as being genuine by first providing a storage medium, preferably machine readable, such as by printing a magnetic composition (e.g. ink) onto a part of the irregular surface of the item so as to form a storage area on the document. The document (item-of-value) will generally be made of a fibrous medium, such a paper, which exhibits a highly irregular surface contour characteristic. In the case of a magnetic stripe, a magnetic composition, used to form the magnetic stripe, will flow over and follow the irregular surface giving the resultant magnetic storage stripe a highly irregular geometry, surface contour and magnetic particle concentration characteristic resulting in a non-uniform, difficult to read, magnetic flux characteristic along the stripe.

Brief Summary Text (18):
The resulting recovered portion of the bit string which is the encrypted identifier, is then decrypted and compared with the obtained verification value according to a predefined compare criterion. The item is authenticated when the verification value and the decrypted identifier value compare according to the predefined compare criterion. The verification value and the decrypted identifier do not need to match exactly for the document's authenticity to be assured. The number of errors which can be accepted and still result in a positive authentication indication are predefined and are part of the predefined compare criterion.

Detailed Description Text (12):
In a preferred embodiment of the invention, encryption of the identifier occurs using a private key while decryption is done using a public key. In accordance with the teaching of U.S. Pat. No. 4,405,829, successful decryption according to the public key evidences the authenticity of the document by establishing that the document originated from a particular source since decryption using the public key designation would only be possible if encryption had occurred in accordance with a private key known only to the legitimate originator of the document.

Current US Cross Reference Classification (1):
340/5.86

CLAIMS:

1. A method for authenticating a printable item made of a medium subject to physical damage and having an irregular random surface and a machine-readable uniqueness characteristic over a specified are of the item, the method comprising the steps of:

applying a magnetic composition onto a part of the irregular surface of the item, the magnetic composition forming a magnetic stripe having a non-uniform magnetic characteristic along the surface of the item;

encoding the item according to the substeps of:

reading the uniqueness characteristic along the specified area of the item to define an identifier;

writing the identifier value onto the magnetic stripe to thereby encode the item; and

authenticating the encoded item according to the substeps of:

reading the uniqueness characteristic along the specified area of the item to obtain a verification value;

reading the magnetic stripe to obtain the identifier written thereon by substeps of:

sensing the magnetic flux variations along the magnetic stripe and generating therefrom an analog data signal characterized by peaks in the analog data signal;

conditioning the analog data signal by obtaining a uniform amplitude of the peaks and filtering of noise from the signal;

detecting the position of the peaks, whether of negative or positive polarity, of the conditioned analog data signal;

sensing the differential position between successive peaks;

sensing the polarity of each peak;

processing the differential positions and polarity information to assign a first value representative of a "0" to a bit when there is a first differential position value, to assign a second value representative of a "1" when there is a second differential position value, to assign a third value representative of a non-data character when there is a third differential position value, and assigning values other than the first, second or third values to peaks whose differential position is other than the first, second or third differential positions;

recovering the values of the data bits whose value could not be defined in the step of processing by applying predefined error correction criteria to a data bit string of the assigned values; and

comparing the verification value and the identifier read from the magnetic stripe according to a predefined comparison criterion, the item being authenticated when the verification value and the read identifier compare according to the predefined comparison criterion.

3. The method of claim 2 wherein the step of authentication comprises a further substep decrypting the encrypted identification value stored on the magnetic stripe according to a decryption key prior to comparing the decrypted identifier with the verification value to authenticate the item.

4. A method for authenticating a printable item made of a medium subject to physical damage and having an irregular random surface and a machine-readable uniqueness characteristic over a specified area of time, the method comprising the steps of:

applying a magnetic composition onto a part of the irregular surface of the item, the magnetic composition forming a magnetic stripe having a non-uniform magnetic characteristic along the surface of the item;

encoding the item according to the substeps of: reading the uniqueness characteristic along the specified area of the item to define an identifier;

writing the identifier value onto the magnetic stripe to thereby encode the item by substeps of:

defining a first string of bits each bit having a value of "1" or "0" representative of a data bit string;

defining a second string of bits each bit having a value of "1" or "0" representative of a start sentinel;

defining a third string of bits, each bit having a value of "1" or "0" representative of a stop sentinel;

representing each bit of the first, second and third string of bits by a predefined time period between flux changes along the magnetic stripe, a "0" being represented by a first time period and a "1" being represented by two consecutive second time periods, each second time period equal to 1/2 the duration of the first time period;

defining a framing character having two consecutive third time periods, each equal to 3/2 the duration of the first time period;

effecting magnetic flux changes along the magnetic stripe in accordance with the time period representation for "1's", "0's" and framing characters to store first the second string, next the first string and last the third string, with framing characters being interposed at predefined intervals in the first string; and

authenticating the encoded item according to the substeps of:

reading the uniqueness characteristic along the specified area of the item to obtain a verification value;

reading the magnetic stripe to obtain the identifier written thereon; and

comparing the verification value and the identifier read from the magnetic stripe according to a predefined comparison criterion, the item being authenticated when the verification value and the read identifier compare according to the predefined comparison criterion.

6. The method of claim 5 wherein the step of authentication comprises a further substep of decrypting the encrypted identification value stored on the magnetic stripe according to a decryption key prior to comparing the decrypted identifier with the verification value to authenticate the item.

Previous Doc Next Doc Go to Doc#

L21: Entry 12 of 16 File: USPT Nov 15, 1988

DOCUMENT-IDENTIFIER: US 4785290 A
TITLE: Non-counterfeitable document system

Application Filing Date (1):
19870430

Brief Summary Text (2):
A growing need exists for a practical system of identification for use in various specific applications to segregate counterfeits, imitations or fakes from genuine articles. Regarding commercial products, several indicators suggest that ever increasing numbers of fakes are appearing in a wide variety of different merchandise lines. The piracy of recorded material, e.g. phonograph records, audio tapes, and video tapes, has been a recognized problem for some time. However, the practice of marketing fakes now has grown to encompass many other products. Successful products bearing prestigious trademarks are copied in detail for fraudulent sales. Unfortunately, although legal remedies often exist to curtail the sales of such counterfeits, detection and enforcement often is difficult and expensive. To compound the problem, many fakes cannot be readily detected without careful study or inspection by a professional. In view of the various difficulties and the existing conditions, a considerable need exists for an economical, practical system to verify or authenticate genuine articles both in the interests of preserving trademark or brand integrity and protecting the public from fraudulent copies.

Brief Summary Text (4):
Individual serial numbers or other identifications have also been applied to products for the purpose of authentication. Yet, failing either complete cooperation from sales people, or a comprehensive detection and policing program, such techniques afford little protection against copies. As a result of such difficulties, product pirates have been relatively free to pick and choose from a current group of successful products that could be copied, the fakes to be sold on a global scale with relative impunity.

Brief Summary Text (5):
In addition to commercial products, authentication is important in a variety of other applications as for commercial paper, identification cards, documents of value, and so on. As disclosed herein, the system of the present invention may be variously implemented to authenticate a wide range of subjects, including people.

Brief Summary Text (6):
The present invention is based on recognizing that an effective system of authentication can utilize a device with an obscure random characteristic. The system also recognizes that objects with such characteristics are readily available so that authentication devices hereof can be produced and used inexpensively, enabling selective investigation. For example, a producer can provide his fullline of products with an authenticator, then limit policing activities to either sample groups or those select, very successful products that are most likely to be copied.

Brief Summary Text (12):

As disclosed in detail below, the system hereof may be variously implemented using different media and techniques. For example, the location of the random pattern of concern may be visually obscure and can be crytographically encoded by a computer apparatus. Also, the characteristic reference signals can be variously stored for future comparisons. Some or all of such signals might be kept on a list, or cryptographically encoded and recorded, in memory, or optically or magnetically on the authenticator media.

Drawing Description Text (3):
FIG. 1 is a perspective view of an authenticator tag according to the present invention illustrated for use in association with a product;

Detailed Description Text (3):
Referring initially to FIG. 1, a shoe S is fragmentarily represented along with an authenticator tag T which is securely attached to the shoe by a cord C. The tag T carries a legend in the form of a reference number 10 which may be duplicated in the shoe, e.g. number 12. In general, the system of the present invention enables authentication of the tag T to verify that the shoe S is a genuine article. First, the tag T is identified with the shoe S by the similar numbers and 12. However, more significantly, the number 10 indicates and specifies a measurable but not practicably duplicable physical characteristic of the tag T. Specifically, in a space 14 (generally designated on the tag T) a field of locations (array of squares) is defined (not actually marked in detail) which has a characteristic measurable, but not practicably duplicable pattern of variations in translucency. The location of that pattern and its form are defined by a representative number that is cryptographically related to the identical numbers 10 and 12. That is, a pattern of locations in the space 14 and their translucency are coded into the reference number 10.

Detailed Description Text (4):
It is to be realized that the tag T (if authentic) verifies the genuine nature of the particular shoe S only because the identification numbers 10 and 12 coincide. For an alternative more direct authentication, the medium of the space 14 may be integrated in the actual product that is to be identified, or other codes can be employed. For example, in the case of art work, e.g., signed graphic prints, a marginal area of the sheet of paper bearing the print may serve to provide the pattern of measurable but not duplicable random variations. For other products, other characteristics can be utilized. However, note that a specific tag T may be employed only to identify a single article. That is, while the tag T might be affixed to a fake duplicate of the shoe S, such a switch to the counterfeit shoe would leave the genuine shoe S without an authenticator thereby presumably reducing its value.

Detailed Description Text (5):
In alternative implementations, the tag T might be completely blank or could carry only an indication of the coded locations. In such implementations, the pattern locations could be uniform and the information on the characteristic pattern could be kept on an inventory or list of specific products or objects. Comparing a freshly sensed characteristic pattern with the recorded characteristic pattern would then authenticate a product. Such implementations could be desirable for items of limited production or large monetary value, e.g., graphic art prints.

Detailed Description Text (20):
The word PN is completed with miscellaneous data as indicated above and reduced to the form of the reference number 10 which is printed on the authenticator tag T. The tag T is then available for authentication to verify the likelihood that an associated product is genuine without reference to other memory. Thus, it is not necessary in this implementation to store inventories of tag characteristic data separate from the tags themselves.

Detailed Description Text (21):
In the authentication or test operation, the authentication system of this embodiment cryptographically decodes a portion of number 10 (code word CW) to provide the decoded word DW. That word indicates: the precise location of the observed pattern of squares 29 in the array 28 (FIG. 5) and the digits indicative of the previously observed value of the physical characteristic at each of such individual squares.

Detailed Description Text (35):
The register 60 may incorporate a readout device for providing the reference number 10 (representative of word PN). Alternatively, the signals representative of the number may be employed to drive any of a variety of printing mechanisms to imprint the identification number on the tag authenticators T. If desired, as indicated above, the identification number may also be placed on the article or product for sale (number 12, FIG. 1). In an another arrangement, the PN register 60 may be connected to a magnetic recorder 64 for recording the number PN on the authenticator it identifies, the authenticator incorporating a magnetic recording surface as disclosed in detail below. A system of continuous operation for producing complete authenticators also is described below.

Detailed Description Text (36):
After an authenticator, e.g. tag T (FIG. 1) is associated with an article, e.g. the shoe S, in due course the occasion may arise to verify the authenticity. In general, verification is performed by reading the number 10 (word PN) and decoding it to obtain: (1) the locations of squares 29 in the space 14 which are to be sensed (word AN) and (2) the values of the characteristic expected to be sensed at the indicated squares (word CC). With such information, the array 28 is defined (FIG. 5) then the identified squares (FIG. 6) are sensed. The resulting fresh numerical observations (word CC') then are compared with the similar previous recorded observations (word CC) to confirm authenticity.

Detailed Description Text (43):
Considering various degrees of comparison which may be sensed as disclosed in the system of FIG. 8, the material of the authenticator and its environment may permit use to a standard of complete coincidence. However, with regard to other products, considerable tolerance may be advisable to allow for damage to a portion of the authenticator. In that regard, tests on various fibrous materials including paper tag or label stock indicate a wide variety of media that meet the requirement of being repeatably scannable, preservable, and unique with regard to the translucency patterns discussed above.

Detailed Description Text (75):
In an alternative implementation, deemed suitable for small production articles, the characteristic codes of authenticators may be registered in computer memory for test verification. Specifically, an authenticator (paper for example) could be measured or sensed to provide a characteristic code word for a product. The code word would then be placed on a list to be scanned for verifying an authenticator accompanying the product. Various other implementations will be apparent, including forms where part or all of the code word is carried with the product and can be obscured as disclosed in detail above, by cryptographic encoding. The pattern of predetermined squares may also be preserved in secrecy as disclosed in the above detailed embodiment. Of course, various forms of energy, record medium and so on may be employed in the system. In addition to paper, certain forms of card stock also have been found to be appropriate as being repeatably scannable, preservable and unique. As suggested above, spectral response variations may also be used for further assurance against counterfeits.

Current US Original Classification (1):
340/5.86

Current US Cross Reference Classification (1):
235/380

Current US Cross Reference Classification (4):
380/54

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 9 of 9 returned.

☐ 1. Document ID: US 6600823 B1

Using default format because multiple data bases are involved.

L25: Entry 1 of 9 File: USPT Jul 29, 2003

US-PAT-NO: 6600823
DOCUMENT-IDENTIFIER: US 6600823 B1

TITLE: Apparatus and method for enhancing check security

DATE-ISSUED: July 29, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hayosh; Thomas D.	Bloomfield Hills	MI		

US-CL-CURRENT: 380/51; 380/55, 713/170, 713/176, 713/179

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☐ 2. Document ID: US 5640002 A

L25: Entry 2 of 9 File: USPT Jun 17, 1997

US-PAT-NO: 5640002
DOCUMENT-IDENTIFIER: US 5640002 A

TITLE: Portable RF ID tag and barcode reader

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☐ 3. Document ID: US 5303370 A

L25: Entry 3 of 9 File: USPT Apr 12, 1994

US-PAT-NO: 5303370
DOCUMENT-IDENTIFIER: US 5303370 A

TITLE: Anti-counterfeiting process using lenticular optics and color masking

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☐ 4. Document ID: US 4807287 A

L25: Entry 4 of 9 File: USPT Feb 21, 1989

US-PAT-NO: 4807287
DOCUMENT-IDENTIFIER: US 4807287 A

TITLE: Document authentication method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 5. Document ID: US 4785290 A

L25: Entry 5 of 9 File: USPT Nov 15, 1988

US-PAT-NO: 4785290
DOCUMENT-IDENTIFIER: US 4785290 A

TITLE: Non-counterfeitable document system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 6. Document ID: US 4663622 A

L25: Entry 6 of 9 File: USPT May 5, 1987

US-PAT-NO: 4663622
DOCUMENT-IDENTIFIER: US 4663622 A

TITLE: Non-counterfeitable document system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 7. Document ID: US 4546352 A

L25: Entry 7 of 9 File: USPT Oct 8, 1985

US-PAT-NO: 4546352
DOCUMENT-IDENTIFIER: US 4546352 A
** See image for Certificate of Correction **

TITLE: Non-counterfeitable document system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 8. Document ID: US 4489318 A

L25: Entry 8 of 9 File: USPT Dec 18, 1984

US-PAT-NO: 4489318
DOCUMENT-IDENTIFIER: US 4489318 A
** See image for Certificate of Correction **

TITLE: Non-counterfeitable document system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

☐ 9. Document ID: US 4423415 A

L25: Entry 9 of 9 File: USPT Dec 27, 1983

US-PAT-NO: 4423415
DOCUMENT-IDENTIFIER: US 4423415 A
** See image for Certificate of Correction **

TITLE: Non-counterfeitable document system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L24 and L21	9

Display Format: - Change Format

Previous Page Next Page Go to Doc#

A+

no tag/label

L4: Entry 2 of 9 File: USPT May 2, 2000

US-PAT-NO: 6058481
DOCUMENT-IDENTIFIER: US 6058481 A

TITLE: Smart cards

DATE-ISSUED: May 2, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kowalski; Jacek	Les Jardins des Seignieres			FR

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Inside Technologies	Saint Clement les Places			FR	03

APPL-NO: 09/ 043761 [PALM]
DATE FILED: March 26, 1998

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
FR	95 12176	October 9, 1995

PCT-DATA:

APPL-NO	DATE-FILED	PUB-NO	PUB-DATE	371-DATE	102(E)-DATE
PCT/FR96/01541	October 1, 1996	WO97/14120	Apr 17, 1997	Mar 26, 1998	Mar 26, 1998

INT-CL: [07] G09 C 3/08

US-CL-ISSUED: 713/201; 713/168, 380/255
US-CL-CURRENT: 713/201; 380/255, 713/168

FIELD-OF-SEARCH: 380/255, 380/268, 713/161, 713/168, 713/179, 713/201

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4218738	August 1980	Matyas et al.	380/25
☐	4827450	May 1989	Kowalski	365/185

☐	4847890	July 1989	Solomon et al.	379/67
☐	4868489	September 1989	Kowalski	324/61P
☐	4881199	November 1989	Kowalski	365/189.01
☐	4916333	April 1990	Kowalski	307/296.5
☐	4962449	October 1990	Schlesinger	713/200
☐	4962532	October 1990	Kasiraj et al.	380/25
☐	5022001	June 1991	Kowalski et al.	365/185
☐	5060198	October 1991	Kowalski	365/201
☐	5060261	October 1991	Avenier et al.	380/3
☐	5097146	March 1992	Kowalski et al.	307/350
☐	5191498	March 1993	Kowalski	361/1
☐	5291434	March 1994	Kowalski	365/96
☐	5327018	July 1994	Karlish et al.	307/244
☐	5381452	January 1995	Kowalski	377/26
☐	5394359	February 1995	Kowalski	365/185
☐	5420412	May 1995	Kowalski	235/492
☐	5442589	August 1995	Kowalski	365/225.7
☐	5444412	August 1995	Kowalski	327/541
☐	5448187	September 1995	Kowalski	326/81
☐	5473564	December 1995	Kowalski	365/185.1
☐	5512852	April 1996	Kowalski	327/206
☐	5534686	July 1996	Kowalski et al.	235/492
☐	5550919	August 1996	Kowalski	380/23
☐	5552621	September 1996	Kowalski	257/321
☐	5576989	November 1996	Kowalski	365/185.09
☐	5721440	February 1998	Kowalski	257/300
☐	5740403	April 1998	Kowalski	395/491

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 409 701	January 1991	EP	
2164939	August 1973	FR	
2471003	June 1981	FR	
WO 92/06451	April 1992	FR	
WO 92/15096	September 1992	FR	
WO 92/15074	September 1992	FR	
2698195	May 1994	FR	
WO 94/11829	May 1994	FR	

ART-UNIT: 277

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Nilles & Nilles, S.C.

ABSTRACT:

A logic machine and a circuit for producing an authentication code for authenticating smart cards which include a cycle of steps wherein a bit word is read out of a secret memory with a plurality of bit words, and words read out during previous cycles are combined. The result of the combination is used as a generator word for generating the address of the word to be read out in the next cycle.

11 Claims, 7 Drawing figures

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

L4: Entry 2 of 9 File: USPT May 2, 2000

DOCUMENT-IDENTIFIER: US 6058481 A
TITLE: Smart cards

Application Filing Date (1):
19980326

Detailed Description Text (7):
Thus, if a number n of clock pulses H is applied after a reset to zero of the logic machine 20, the output of the circuit 22 provides, at the n.sup.th clock pulse H.sub.n, a binary word GA generating the address of the word to be read out at the following clock pulse H.sub.n+1 which is the result of the combination of the words M.sub.1, M.sub.2, M.sub.3, M.sub.4, . . . M.sub.n read out of the memory 21 since the first clock pulse. The word GA can be expressed by:

Detailed Description Text (38):
Although it has been indicated in the preamble that the purpose of the present invention is to improve smart cards, it is of course obvious that the method and the authentication circuit according to the present invention are suitable for numerous applications and generally relate to any product using a wired-logic microcircuit whose authenticity has to be verified, like contactless electronic tags (operating by means of electromagnetic signals), electronic keys (with or without contact), electronic cards for the identification of persons, etc.

Previous Doc Next Doc Go to Doc#

L4: Entry 1 of 9 File: USPT Nov 28, 2000

US-PAT-NO: 6152367
DOCUMENT-IDENTIFIER: US 6152367 A

TITLE: Wired logic microcircuit and authentication method having protection against fraudulent detection of a user secret code during authentication

DATE-ISSUED: November 28, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kowalski; Jacek	Les Jardins des			FR

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Inside Technologies	Saint Clement les Places			FR	03

APPL-NO: 09/ 043762 [PALM]
DATE FILED: March 26, 1998

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
FR	95 12178	October 9, 1995

PCT-DATA:

APPL-NO	DATE-FILED	PUB-NO	PUB-DATE	371-DATE	102(E)-DATE
PCT/FR96/01524	October 1, 1996	WO97/14119	Apr 17, 1997	Mar 26, 1998	Mar 26, 1998

INT-CL: [07] G06 K 5/00

US-CL-ISSUED: 235/382; 235/380
US-CL-CURRENT: 235/382; 235/380

FIELD-OF-SEARCH: 235/382, 235/380, 235/375, 235/379

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4295039	October 1981	Stuckert	235/380
☐	4710613	December 1987	Shigenaga	235/380

☐	4802218	January 1989	Wright et al.	380/23
☐	4827450	May 1989	Kowalski	365/185
☐	4864618	September 1989	Wright et al.	380/51
☐	4868489	September 1989	Kowalski	324/61P
☐	4881199	November 1989	Kowalski	365/189.01
☐	4900903	February 1990	Wright et al.	235/308
☐	4900904	February 1990	Wright et al.	235/381
☐	4916333	April 1990	Kowalski	307/296.5
☐	5022001	June 1991	Kowalski et al.	365/185
☐	5060198	October 1991	Kowalski	365/201
☐	5060261	October 1991	Avenier et al.	380/3
☐	5097146	March 1992	Kowalski et al.	307/350
☐	5120939	June 1992	Claus et al.	235/382
☐	5191498	March 1993	Kowalski	361/1
☐	5291434	March 1994	Kowalski	365/96
☐	5327018	July 1994	Karlish et al.	307/244
☐	5381452	January 1995	Kowalski	377/26
☐	5394359	February 1995	Kowalski	365/185
☐	5420412	May 1995	Kowalski	235/492
☐	5442589	August 1995	Kowalski	365/225.7
☐	5444412	August 1995	Kowalski	327/541
☐	5448187	September 1995	Kowalski	326/81
☐	5473564	December 1995	Kowalski	365/185.1
☐	5512852	April 1996	Kowalski	327/206
☐	5534686	July 1996	Kowalski et al.	235/492
☐	5550919	August 1996	Kowalski	380/23
☐	5552621	September 1996	Kowalski	257/321
☐	5576989	November 1996	Kowalski	365/185.09
☐	5577121	November 1996	Davis et al.	380/24
☐	5657388	August 1997	Weiss	380/23
☐	5721440	February 1998	Kowalski	257/300
☐	5740403	April 1998	Kowalski	395/491
☐	5892211	April 1999	Davis et al.	235/380

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 028 965	May 1981	EP	

0 029 894	June 1981	EP
0 427 465	May 1991	EP
2650097	January 1991	FR
2698195	May 1994	FR
2144564	March 1985	GB
WO 92/06451	April 1992	WO
WO 92/15096	September 1992	WO
WO 92/15074	September 1992	WO
WO 94/11829	May 1994	WO

ART-UNIT: 286

PRIMARY-EXAMINER: Hajec; Donald

ASSISTANT-EXAMINER: Fureman; Jared J.

ATTY-AGENT-FIRM: Nilles & Nilles SC

ABSTRACT:

An authentication method for a wired-logic microcircuit mounted on a support and a microcircuit reading terminal. The microcircuit is provided with a memory which has data readable by the terminal. A secret code of the microcircuit is arranged in a region of the memory that is not readable by the terminal. The microcircuit generates an authentication code from the data in the memory that is readable by the terminal, the secret code and a random code. The terminal generates an authentication code from the data in the microcircuit memory that is readable by the terminal, a secret code provided to the terminal by a microcircuit user and random code, and the authentication code generated by the microcircuit is compared with the authentication code generated by the terminal.

21 Claims, 3 Drawing figures

Previous Doc Next Doc Go to Doc#

L4: Entry 1 of 9 File: USPT Nov 28, 2000

DOCUMENT-IDENTIFIER: US 6152367 A
TITLE: Wired logic microcircuit and authentication method having protection against fraudulent detection of a user secret code during authentication

Application Filing Date (1):
19980326

Detailed Description Text (14):
For security reasons, the injection of NI and DA as components of the input code CE allows the setting of the authentication circuit 52 to an internal logic state as far as possible from its logic state "zero", i.e. the logic state after the reset to zero of the circuits that it comprises.

Detailed Description Text (17):
Step 4: the switching units 56 and 57 are set in the position P4/PS, the input of the authentication circuit 52 being thus connected to the input-output pin I/C. A conventional procedure, which is known per se, begins for authenticating the card. Because this procedure has been preceded by the steps 1 to 3 according to the invention, it can consist in several alternatives, depending on the fact that the authentication circuit 52 is reset to zero or left in the internal logic state that it had at the end of step 3.

Detailed Description Text (18):
(a) If the circuit 52 is reset to zero, it can be provided that the terminal 10, which has already read the data NI and DA in step 1, sends back NI and DA to the authentication circuit 52 together with a random code ALEXT produced by itself.

Detailed Description Text (19):
(b) If the authentication circuit 52 is not reset to zero, the terminal sends the random code ALEXT only, it is no more necessary to send back the data NI and DA to the authentication circuit 52 which has already received them in step 1.

Detailed Description Text (58):
Generally, the present invention relates to any product using a wired-logic microcircuit whose authenticity has to be verified, like contactless electronic tags (operating by means of electromagnetic signals), electronic keys (with or without contact), electronic cards for the identification of persons, etc.

g) comparison means comparing said first digital signal with a predetermined second digital signal to within a predetermined tolerance; and

h) output means indicating a positive authentication result if said first and second digital signals agree to within said tolerance, and otherwise indicating a negative authentication result.

15. An authentication system for discriminating among articles marked with one or more fluorescent substances which emit fluorescent light in response to electromagnetic radiation, comprising:

a) a source of electromagnetic radiation in at least one of the ultraviolet, visible, and infrared spectral ranges;

b) a driver circuit adapted to energize said source at a predetermined frequency, said driver circuit further comprising at least one crystal, and said predetermined frequency being determined by said at least one crystal;

c) first optical means for transmitting said electromagnetic radiation from said source toward said articles;

d) second optical means for transmitting said fluorescent light toward at least one detector capable of producing a first analog signal responsive to said fluorescent light, said first and second optical means being adapted to be substantially coaxial;

e) wavelength-selective means disposed to allow selected portions of said spectral ranges to illuminate said detector;

f) amplifier means adapted to synchronously detect said first analog signal at said predetermined frequency;

g) an electrical bandpass filter adapted to pass said predetermined frequency and to remove selected other frequencies from said first analog signal to produce a second analog signal;

h) an analog-to-digital converter converting said second analog signal to a digital signal,

i) a computer operating under a predetermined program and comparing said digital signal to one or more predetermined digital signals, said computer being adapted to discriminate between said marked articles and other articles not so marked, and

j) digital output means responsive to said computer to indicate authentication or lack of authentication of said articles to be discriminated.

Previous Doc Next Doc Go to Doc#

L21: Entry 8 of 16 File: USPT Aug 13, 1996

DOCUMENT-IDENTIFIER: US 5546463 A
TITLE: Pocket encrypting and authenticating communications device

Abstract Text (1):
A portable security device is disclosed which can be carried by an individual and connected directly to telephone circuits to both authenticate that individual and encrypt data communications. The invention can operate as an electronic "token" to uniquely identify the user to a network, to a computer system or to an application program. The "token" contains the complete network interface, such as a modem, which modulates the data and provides the circuitry required for direct connection to the network. Furthermore, this "token" will not permit communications to proceed until the device, and optionally the user, have been identified by the proper authentication. The token also contains all of the cryptographic processing required to protect the data using data encryption or message authentication or digital signatures or any combination thereof. Thus, the present invention provides the user with all of the communications and security equipment needed for use with personal computers and electronic notebooks and eliminates the need for any other security measures and/or devices.

Application Filing Date (1):
19940712

Brief Summary Text (2):
This invention relates to a complete and transportable security device having a network communications interface which provides encryption and authentication capabilities to protect data and restrict access to authorized users. The device can be carried by the user in a pocket or a purse.

Brief Summary Text (7):
U.S. Pat. No. 4,546,213 describes a modem security device, but the device does not provide efficient encryption and authentication capabilities nor can it be carried as a "token" to control access to a computer network. Several methods of "authenticating" the user using "biological" attributes, such as fingerprint readers, retina (eye) scanners are known. For example, U.S. Pat. No. 5,153,918 describes a security system for data communications for securing access to a computer system using voice recognition as the access control medium. Similarly, Young and Hammon in U.S. Pat. No. 4,805,222 describe the use of operator keystroke dynamics to identify the user. Unfortunately, these methods have proven to be expensive for ordinary commercial use and have been considered to be inconvenient or intrusive by potential users.

Brief Summary Text (8):
Lessin, U.S. Pat. No. 4,868,376, incorporates a means of authenticating a user with a personal identification number (PIN). The Lessin security device is contained in a portable housing, such as a smartcard, but requires connection to a non-portable reader and does not include means for direct connection with a telephone network. U.S. Pat. No. 5,301,234 describes a radiotelephone installation for prepayment operation with security protection using encryption to authenticate the device, but the '234 reference discloses use of the device in conjunction with payment of services for radiotelephone sets--not digital communications security with data

encryption. U.S. Pat. No. 5,239,294 describes a means of authenticating a subscriber's device to control access to cellular telecommunications networks, but is specifically directed to use with radio telecommunication systems.

Brief Summary Text (11):
The present invention is a transportable authenticating and encrypting device which includes an encryptor for encrypting data received by the device, an authenticator for authenticating use of the device by a user, and a modem for transmitting the data and for receiving the data over a data transfer path, such as a telephone line. The encryptor, authenticator, and modem can be co-located in a compact housing whereby the device can be conveniently transported on the person of the user in a discrete manner, such as in the pocket or purse of the user.

Brief Summary Text (13):
The authenticator is preferably a cryptographic means which identifies the authorized user by an authorized user identification such as a message authentication code or digital signature.

Brief Summary Text (15):
The portable encryption and authentication device preferably employs the use of a keypad mounted on the housing to enter a personal identification number (PIN). The authenticator can also be operated by the insertion of a smartcard which contains a pin or code which uniquely identifies the user.

Brief Summary Text (16):
Preferably, the compact authenticating and encryption device includes a means of detecting the modification of messages sent or received by message authentication codes or digital signatures.

Brief Summary Text (17):
Also, preferably, the keys used for encryption and the keys used for authentication may be changed from a remotely located key management center or by another authorized encryption device.

Brief Summary Text (19):
The present invention is a device which incorporates the use of encryption and authentication techniques uniquely with a communications interface device, such as a modem. The device is portable and can replace an entry means (such as a token) to identify the user and protect communication from unwanted eavesdropping.

Brief Summary Text (21):
These advantages have been met by incorporating into a portable-sized housing the combination of a highly secure message encryptor and user authenticator. This device serves as an entry token which can be assigned to an individual and easily transported by that person in a pocket or purse and uniquely identifies that person to another such cryptographic device.

Brief Summary Text (23):
Furthermore, as a result of the present invention, the operation and setup of otherwise complex and sophisticated equipment is simplified significantly. This has been done by eliminating configuration and cabling requirements and adjustments usually associated with discrete modem, encryptor, and authenticator components.

Brief Summary Text (24):
Moreover, as a result of the architecture provided herein, communications must be passed through the proper cryptographic protection in order to order to provide access to the user. Moreover, protection cannot be defeated either through accidently bypassing connections to the encryptor or by mere neglect. Furthermore, encryption and authentication services can be provided for software application.

Drawing Description Text (3):
FIG. 1A is a perspective view of a compact authenticating/encrypting device in accordance with the present invention;

Drawing Description Text (4):
FIG. 1B is a perspective view of a card-size embodiment of an encrypting/authenticating device according to the invention;

Drawing Description Text (8):
FIG. 4A is a diagram of the flow of data within the encrypting and authenticating device of the present invention, which shows the processing sequence for in-line mode of encryption and authentication;

Drawing Description Text (9):
FIG. 4B is a diagram of the flow of data within the encrypting and authenticating device of the present invention which shows the processing sequence for off-line mode of encryption and authentication;

Detailed Description Text (2):
The present invention is a portable device which can be used as an identifying token, a communications network interface, a data encryptor, and a user authenticator. It provides an electronic token which can be carried by the user to uniquely identify him or her to a network, to a computer system or to an application program. The device contains the modem which modulates the data in such a way that it can be directly connected to a data transfer path, such as telephone network. The device will not permit communications to proceed until such device and, optionally, the user, have been identified by the authenticator. The device also contains all of the cryptography required to protect the data using data encryption or message authentication or digital signatures or any combination thereof. Thus, the present invention provides the user with all of the communications and security equipment needed for use with personal computers and electronic notebooks and eliminates the need for any other security apparatus. The device is a complete service interface/security device which makes complete communications security practical when used with portable computing equipment.

Detailed Description Text (4):
Referring to FIG. 1A, the encrypting/authenticating device 10 is depicted in a single housing 11 of convenient size which may be physically protected from unauthorized tampering. It is possible to use a potting compound having solvents which cause damage to electronic components, making the device inoperable.

Detailed Description Text (7):
FIG. 1B illustrates another embodiment of the encrypting/authenticating device 10', except that the physical manifestation is a card, similar in length and width to a credit card. One connector 12 is a standard female receptacle known to the art as a PCMICA connector which can be directly connected to any personal computer with a corresponding connector. Another connector 14 is a modular receptacle for direct cable connection to a telephone system.

Detailed Description Text (8):
FIG. 1C depicts a device 10" in accordance with the invention which is designed to receive a smartcard 19 in receptacle 18. The smartcard 19 and device 10" operate cooperatively as an encrypting/authenticating device.

Detailed Description Text (9):
FIG. 2 is a block diagram of the major components of the encrypting/authenticating device 10, showing connectors 12 and 14, and use of a microprocessor bus to control internal functions. Referring to FIG. 2, a microprocessor 24, RAM 26 and ROM 28 execute a program to control the encryption, authentication and modem functions. The modem 30, encryptor 32 and communications port 34 respond to control signals to

provide the cryptographic functions. The encryptor 32 provides a cryptographic function, such as by signal, punch-board, algorithms, etc., and procedures which can be executed in a microprocessor. These functions can also be accomplished by use of a set of available commercial encryption chips which are designed to interface with a microprocessor. The encryption function is used to perform data encryption as well as all of the forms of authentication described herein. The embodiment illustrated in FIG. 2 is not necessarily descriptive of the physical circuit components because many of the functions can be integrated into common physical packages. For example, the communications port 34 may be an integral part of the microprocessor chip 24. Similarly, the encryptor 32 may be performed by the firmware of the microprocessor 24 and its memory and, therefore, not actually implemented as a separate integrated circuit chip.

Detailed Description Text (10):
The operation of the device with respect to data encryption, device authentication, user authentication and message authentication will now be described. Specifically, FIG. 6 shows the encryption and decryption of communications data. Both the encrypt and decrypt functions are employed so that messages can be both sent and received. Plaintext data 72 is encrypted (Block 74) using a plurality of encryption algorithms well known to practitioners such as Feistel, U.S. Pat. No. 3,798,359 or Rivist, U.S. Pat. No. 4,405,829. The cryptographic algorithms used to perform these functions may be chosen from a variety of standard algorithms, usually in conformance with federal or national standards, and do not need to be described here in further detail. The choice of algorithm is unimportant to this invention. For example, encryption and decryption could be performed in accordance with American National Standard (ANS) X3.92, Data Encryption Standard, or by the Federal Information Processing Standard 185, Escrow Encryption Standard. The encrypted data is rendered unintelligible and therefore is kept confidential when it appears on the communications line 78. The data is received (Block 80) and sent to a decryption function using a decryption algorithm which corresponds to the encryption algorithm described above and which recovers at output 84 the original plaintext 72. The only requirement is that they keys used by these standards for encryption and decryption must correspond and the modes of operation specified in these standards must be that same for encryption (Block 74) and decryption (Block 82).

Detailed Description Text (11):
In addition to encrypting the communicated data as described, above, the communicated data can be authenticated by the sender and verified by the recipient. Data (or message) authentication verifies that data has been received without modification and also verifies the identity of the sender. In FIG. 7, data 90 is transmitted (Block 92) by means of a communications system 94 to a recipient 98. The data is authenticated by a plurality of authentication algorithms well known to the art, all of which process messages and produce an authenticator number or digital signature which is transmitted with the data for use in verifying its source and accuracy. Examples of this process are described in detail in American National Standard X9.9, Message Authentication Standard, or American National Standard X9.30, Digital Signature Standard, or in numerous patents such as U.S. Pat. No. 4,995,082. The result of this authentication process is transmitted (Block 102) to a recipient 104 who performs the verification process (Block 106) to determine if the data 90 has been modified before reception (Block 96). The verification process depends upon the algorithm chosen to implement the present invention. If the authentication was performed in accordance with American National Standard X9.9, for example, then the validation process consists of encrypting the data in block 106 in accordance with the standard and in the same way as was done in block 100 and then comparing the resulting authentication codes with the authentication code which was received 104. If the message was modified in transit or if the keys used to authenticate and validate differ, then with a high degree of probability, the authentication codes will also differ. If digital signatures are used for authentication, then the signing process (Block 100) and the verification

process (Block 106) will use different algorithms which are specified in detail in the appropriate National or Federal standard. In this case, the private key used to sign the data and the public key used to validate it form a set which will correctly validate the data. If a different private key is used to validate the data than the one in the set, then validation with the public key of the set will fail. In this case there is an unambiguous indication that the sender possesses the unique private key and is presumed to be the authorized sender. In any case, the result of the verification decision (Block 108) is provided to the recipient to indicate whether or not the data is valid. This can simply be in the form of a message which describes the accompanying data as being valid or invalid.

Detailed Description Text (17):
The national standards described in this embodiment are examples of common algorithms known to the art and are not the only means of performing the encryption or authentication functions of the present invention. Moreover, analogue and/or digital circuitry can be used to implement the various elements of the present invention.

Detailed Description Text (18):
The two ports of the encrypting/authenticating device 10 described in FIG. 1 are connected in FIG. 3 to a network 20 and a computer or terminal 22. This permits two basic modes of operation:

Detailed Description Text (19):
a) in-line communications in which data transmitted from authenticated user is passed through the device in a single pass and sent in encrypted form to the network through the modem;

Detailed Description Text (20):
b) off-line communications in which data to be transmitted is sent to the device and, after authentication and encryption has been performed, is returned to the user's computer application or terminal for subsequent transmission to the network, possibly as part of another message.

Detailed Description Text (22):
In FIG. 3, the device 10 of the present invention is connected to a network 20 which contains other equipment which provides data encryption, device authentication, user authentication and message authentication services as defined herein. The encryption and authentication component 38 and the modem 40 can be another encrypting and authenticating modem similar to device 10, or can be a collection of commercially available communications security components which are built to compatible standards, as shown in FIG. 3.

Detailed Description Text (23):
In the following discussion, two modes of operation have been addressed, the in-line mode and the off-line mode (sometimes referred to as the attached mode). A set of codes or signals are issued by the user or user's computer to cause the encrypting/authenticating device to switch between these operating modes.

Detailed Description Text (24):
Referring to FIG. 4A, the flow of data through the encrypting/authenticating device in the in-line mode of operation is as follows:

Detailed Description Text (26):
Device authentication, as shown in FIGS. 5A and 5B, is performed by applying an authentication algorithm to a known code, the serial number of the device 56 and a sequence number 58 which increases for each session. The authentication algorithm can be any known to the art, such as ANS X9.9 message authentication code, ANS X9.30 digital signature algorithm (DSA) or ANS X9.31 digital signature algorithm (RSA). Each of these algorithms employ a secret or private key to perform a

cryptographic process upon the items listed above and produce an authenticator code or digital signature. The key 54 used to perform this authentication is held secret so as to prevent others from counterfeiting this code or signature. The result is returned by means of the modem 40 to the sender 38 where it is verified by a procedure described in the authentication standard.

Detailed Description Text (27):
User authentication is an optional procedure which can be invoked at the beginning of the session to ensure that an authorized user or users are in possession of the device. It is performed by sending a time-varying parameter from the remote device 38 to challenge the user. This parameter could take the form of a random number or the time and date, for example, and should not repeat for a long period of time. The encrypting/ authenticating device 10 then may prompt the user for the entry of a password (or PIN) or the insertion of a smartcard containing a unique code to establish his or her identity. The entry is encrypted or used to authenticate a digital signature in accordance with the algorithm selected. The result is returned by means of the modem 40 to the sender of the time-varying parameter 38, for verification.

Detailed Description Text (29):
Once authentication has been successfully completed so that the identities of the device and, optionally, the user have been established, then data encryption (Block 42) and decryption (Block 48) will be allowed to begin. See FIG. 4A. This invention does not permit any of the user's data to pass before authentication is successfully consummated and only passes items such as authentication codes and automatic key management messages requires to securely establish the call. Data may be transmitted by the user's computer or terminal and received at the communications interface 44 of the encrypting/ authenticating device 10 where it is encrypted (Block 42) and passed to a modem function 40 for transmission on a telephone line at connector 14. Data received from the line at the modem 40 will be decrypted (Block 48) and sent by the communications interface 44 to the communications port of the user's computer or modem.

Detailed Description Text (30):
Referring to FIG. 4B, the flow of data through the encrypting/authenticating device 10 in the off-line mode of operation is the same as that described, above, for the in-line mode except that the encrypted data of block 42 is returned to the user's computer or terminal by means of the interface 44 for storage or subsequent transmission by the user. If subsequently transmitted, the data from connector 12 to interface 44 is sent directly to the modem 40 for transmission on the telephone line, bypassing encryption.

Detailed Description Text (32):
Referring to FIG. 7, the internal modem or other communications interface initiates calls when the user issues an industry-compatible modem command to begin dialing. This command is passed directly to the modem as long as no carrier is present on the line. Incoming calls begin with the appearance of carrier on the communications media which causes the modem to raise carrier detect to the microprocessor. In either event, the modem acquires carrier 120 (see FIG. 8) and performs any key establishment which must be performed to initiate a call. This process can simply be the manual loading of a key into the memory of the Pocket Encrypting and Authenticating Device or it could provide for automatic key changes. The selection of method of key entry and management is not important to the description of the present invention as several national standards exist for the management of cryptographic keys, such as American National Standards Institute X9.17. The device then waits for a challenge from the network or other security device. Any security device which meets American National Standard X9.26, for example, will function like FIG. 5A, block 53 and supply this random or time-varying challenge.

Detailed Description Text (34):

After the user has been successfully authenticated as described in the prior paragraph, two concurrent tasks begin to operate, the Inbound Task (see FIG. 9), which processes data from the network, and the outbound task (see FIG. 10), which processes data to the network. Referring to FIG. 9, the Inbound Task simply decrypts (Block 142) data received by the modem and then verifies (Block 146) the data if the message authentication option is enabled. When the call ends and carrier drops, the task is suspended.

Detailed Description Text (36):
Referring to FIGS. 11A and 11B, yet another feature of the present invention is shown which enhances its portability and compactness. In particular, a encrypting/authenticating device 10"' is shown wherein the housing 11"' includes an elongated slot 13 which is provided to accommodate a cable 15 attached to the device to implement the required connections. The slot preferably includes a plurality of projecting ribs 17, which are sized to releasably engage cable 15 when such cable is pressed therebetween. Moreover, the elongated slot 13 can be provided on one or more sides of the housing 10"'. When it is provided on two sides of the housing, the cable 15 can be fed into the slot 13 and rapped continuously around the housing as depicted in FIG. 11B. Another embodiment includes a deeper slot 13 which would accommodate at least a double fold of cable 15 so that it could be extended and returned on a single side of the housing 10"'. Those skilled in the art will be best equipped to design the slot 13 to accommodate the intended use.

Current US Cross Reference Classification (3):
380/30

CLAIMS:

1. An authenticating and encrypting communications device for establishing a secure communications link between a remote computing site and a computing device of a user over a data transfer path, said communications device comprising:

an encryptor for encrypting transmit data to be transmitted to said remote computing site over said data transfer path, and for decrypting receive data received by said communications device from a source;

an authenticator for authenticating to said remote computing site that said communications device is authorized;

a modem for transmitting the transmit data and for receiving the receive data over said data transfer path; and

a compact, pocket-sized housing containing said encryptor, said authenticator and said modem, said encryptor, authenticator and modem being electrically interconnected and being electrically configured for interconnection with said data transfer path and said computing device of said user.

Previous Doc Next Doc Go to Doc#

L21: Entry 10 of 16 File: USPT Apr 12, 1994

DOCUMENT-IDENTIFIER: US 5303370 A
TITLE: Anti-counterfeiting process using lenticular optics and color masking

Abstract Text (1):
An image of a symbol or other indicium of origin or authenticity is encrypted, and printed on the item or a label in superposition with a color mask. In a preferred embodiment, an intermediate parallax record is formed of a series of images of a symbol or other indicium, each differing from the preceding one by a predetermined amount of parallax (i.e. change of viewing angle.) A multiple exposure of the series of intermediate parallax record images is made through a lenticular screen to create the encrypted image of the indicium. The lenticular screen and the medium on which the multiple exposure is made are moved relative to each other between exposures. The encrypted image and the superimposed color mask are then printed as a composite image to produce an unintelligible criss-cross of colored lines. When viewed through a lenticular screen which matches that used to create the encrypted image, the original indicium is revealed in clear form.

Application Filing Date (1):
19921113

Brief Summary Text (10):
Also, none of these systems can be used for authentication of the origin of an item since a skilled operator using a high quality graphic arts camera may be able to create indistinguishable duplicates of the encrypted image which may be applied to counterfeit articles.

Brief Summary Text (14):
In accordance with the invention, an image of a symbol or other indicium of origin or authenticity of the item in question is encrypted, and printed on the item or a label in superposition with a color mask. In a preferred embodiment, an intermediate parallax record is formed of a series of images of a symbol or other indicium, each differing from the preceding one by a predetermined amount of parallax (i.e. change of viewing angle.) The intermediate parallax record is then processed by an optical system including a lenticular screen to create an interlace-encrypted image of the indicium. The encrypted image and the superimposed color mask are then printed as a composite image (which will be referred to for convenience below as an "identifier".) The result is an unintelligible criss-cross of colored lines When the identifier is viewed through a lenticular screen which matches that used to create the encrypted image, the original indicium is revealed in clear form.

Brief Summary Text (15):
The indicium may be a logo or other trademark and the authenticator may be a small plastic card with the required lenticular array molded into it. In one application, where it is desired to protect the origin of collector cards bearing photographs of sports personalities or the like, the encrypted image and the superimposed color mask are printed unobtrusively on the card, and the authenticator is given to collectors or sold at a nominal price.

Brief Summary Text (16):

To verify that the card is genuine, the user views the encrypted image through the authenticator. If the encrypted image has been counterfeited or tampered with, it will be immediately evident, as the image will not be decoded or will appear with superimposed black lines. As a further check on the authenticity of the encrypted image, the color mask may be so arranged that when the authenticator is rotated 90 degrees, the user observes a rainbow pattern, and the image of the indicium returns to its encrypted form.

Brief Summary Text (17):
In another application, the encrypted image and the superimposed color mask are printed on a hang tag or other label which is applied to a branded item. The use of the encrypted identifier is appropriately promoted, and a suitable authenticator is made available for prospective customers who wish to verify that the item they are about to purchase is genuine.

Brief Summary Text (18):
In yet a further application, the principles of the invention are applied to signature verification. For this, the indicium may be a specimen signature of the holder of a checking account or a credit card. The authenticator may be an optical device including a lenticular screen to decode the encrypted image with additional means for side-by-side comparison between the decrypted image and the actual signature on the check or credit transaction record.

Detailed Description Text (45):
It has been determined that the rotation, or orientation of the color bars relative to the scan line of the encrypted image, the width of the colored lines, and the line spacing are important parameters which must be controlled to achieve the desired objectives according to the present invention. For example, if the lines are too wide, or if the angles of intersection .alpha..sub.3 --.alpha..sub.1 (and .alpha..sub.3 --.alpha..sub.2) are tool small, the area covered by the resulting moire pattern will be too large and/or too dark, and the encrypted image will be so completely masked that it cannot be decoded even using a proper authenticator. If the lines are too thin, and/or the intersection angles too large, the interference pattern will be too small or too light, and the susceptibility to unauthorized reproduction will be increased.

Detailed Description Text (49):
Generally speaking, it has been found that the relationship between these various parameters is so complex that for a given interlace-encrypted image, optimization of the color mask parameters by experimentation is necessary. This assures 15 that the resulting areas of intersection are large enough and dark enough to prevent the composite printed image from being copied, but small enough and light enough that viewing the interlace-encrypted image through the authenticator yields a clear image which is unambiguously authentic.

Detailed Description Text (51):
Generally speaking, the values selected for angles .alpha..sub.1 and .alpha..sub.2 affect the appearance of the encrypted image when the authenticator is rotated away from the decrypting position. With larger angles, the "rainbow" effect is more pronounced. This may be desirable for esthetic purposes. Otherwise, values of .alpha..sub.1 and .alpha..sub.2 close to or equal to zero are satisfactory.

Detailed Description Text (56):
Similarly, without knowledge of the exact parameters chosen to create the interlace-encrypted image and the color mask, it is virtually impossible to create an original composite image which will not be revealed as a counterfeit when viewed through the authenticator. Even if the exact parameters are discovered, the effort and cost involved in creating the necessary lenticular screen and color mask so that a counterfeit identifier can be encrypted are generally prohibitive. This assures the authenticity of the article to which the composite image is applied,

and when the system is used for check verification, assures that a counterfeit signature can not be encrypted and applied as the identifier on a check. If the genuine identifier is copied, or a counterfeit original is produced which does not exactly match the genuine identifier, viewing it through the authenticator immediately reveals a distorted image, or one which can not be decrypted at all.

Current US Cross Reference Classification (1):
380/54

Current US Cross Reference Classification (2):
713/176

CLAIMS:

1. A method of authenticating the origin of an item comprising the steps of:

a. Selecting an indicium for identifying the origin of the item;

b. Creating an interlace-encrypted image of the identifying indicium by projecting a succession of images thereof through a lenticular array onto a recording medium for a predetermined exposure interval, and moving the recording medium relative to the lenticular array by a predetermined incremental scan distance between each exposure;

c. creating a color mask comprised of first and second intersecting elements each of a different color; and

d. printing the interlace-encrypted image and the color mask in superposition on the item.

2. An authentication method according to claim 1 further including the step of producing an intermediate parallax record of the selected indicium by creating a series of images thereof, each differing from the prior one by a predetermined amount of parallax, successive ones of the series of images of the intermediate parallax record being used to provide the succession of images projected onto the recording medium to create the interlace-encrypted image.

8. An authentication method according to claim 1 in which the colors are selected such that the density of the areas of intersection of the color elements is approximately equal to or greater than that of the interlace-encrypted image.

10. An authentication method according to claim 9 in which the color mask covers approximately 40% of the area occupied by the interlace-encrypted image when printed on the item.

12. An authentication method according to claim 11 in which the colors are selected such that the density of the areas of intersection of the color elements is approximately equal to or greater than that of the interlace-encrypted image.

13. An authentication method according to claim 11 in which the background color of the field occupied by the lines of the first and second sets and the interlace-encrypted image is of a third color.

16. An authentication method according to claim 15 in which the lines of the second color element are formed to intersect the fourth-color lines, and in which the colors are selected such that the density of the areas of intersection between the lines of the second and fourth colors are of a density approximately equal to or greater than that of the interlace-encrypted image.

19. An authentication method according to claim 18 in which the second color

element is arranged to intersect the fourth color element, and in which the colors are selected so that the density of the intersection of the second and fourth color elements is approximately equal to or greater than the density of the interlace-encrypted image.

20. An authentication method according to claim 18 in which the third element forms a background for the field occupied by the first and second elements and the interlace-encrypted image.

23. An authentication method according to claim 22 in which the lines of the first and third sets are selected to be parallel to the scan direction of the interlace-encrypted image.

24. An authentication method according to claim 21 in which the spacing and width of the line in the first, second, and third sets are selected such that the color mask covers approximately 40% of the field of the interlace-encrypted image when printed on the item.

46. A method of authenticating the origin of an item comprising the steps of:

a. Selecting an indicium for identifying the origin of the item;

b. Creating an encrypted image of the identifying indicium:

c. creating a color mask comprised of first and second intersecting elements each of a different color; and

d. printing the encrypted image and the color mask in superposition on the item.

47. An authentication method according to claim 46 in which the encrypted image is produced by creating a multiple exposure of a succession of images of the indicium projected through a lenticular array onto a recording medium with the recording medium and the lenticular array being moved relative to each other by a predetermined incremental scan distance between each exposure.

50. An authentication method according to claim 46 in which the colors are selected such that the density of the areas of intersection of the color elements is approximately equal to or greater than that of the encrypted image.

53. An authentication method according to claim 52 in which the colors are selected such that the density of the areas of intersection of the color elements is approximately equal to or greater than that of the encrypted image.

54. An authentication method according to claim 53 in which the background color of the field occupied by the lines of the first and second sets and the interlace-encrypted image is of a third color.

57. An authentication method according to claim 56 in which the lines of the second color element are formed to intersect the fourth-color lines, and in which the areas of intersection between the lines of the second and fourth colors are of a density approximately equal to or greater than that of the encrypted image.

60. An authentication method according to claim 59 in which the second color element is arranged to intersect the fourth color element, and in which the colors are selected so that the density of the intersection of the second and fourth color elements is approximately equal to or greater than the density of the encrypted image.

61. An authentication method according to claim 59 in which the third element forms a background for the field occupied by the first and second elements and the

encrypted image.

64. An authentication method according to claim 63 in which the lines of the first and third sets are selected to be parallel to the scan direction of the encrypted image.

Previous Doc Next Doc Go to Doc#